



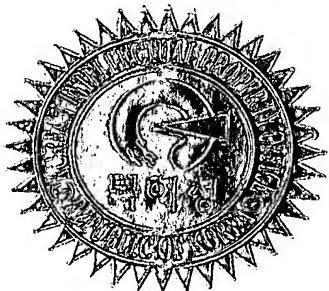
별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto  
 is a true copy from the records of the Korean Intellectual  
 Property Office.

출원번호 : 10-2003-0022981  
 Application Number

출원년월일 : 2003년 04월 11일  
 Date of Application APR 11, 2003

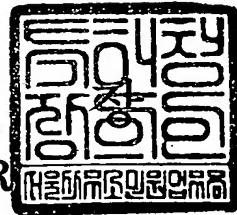
출원인 : 삼성전자주식회사  
 Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 10 월 06 일

특 허 청

COMMISSIONER



## 【서지사항】

【서류명】	특허출원서	
【권리구분】	특허	
【수신처】	특허청장	
【제출일자】	2003.04.11	
【발명의 명칭】	홈 디바이스의 인증시스템 및 그의 인증방법	
【발명의 영문명칭】	Authentication system of home device and a method authenticating thereof	
【출원인】		
【명칭】	삼성전자 주식회사	
【출원인코드】	1-1998-104271-3	
【대리인】		
【성명】	정홍식	
【대리인코드】	9-1998-000543-3	
【포괄위임등록번호】	2003-002208-1	
【발명자】		
【성명의 국문표기】	박상도	
【성명의 영문표기】	PARK, SANG DO	
【주민등록번호】	740302-1074314	
【우편번호】	135-092	
【주소】	서울특별시 강남구 삼성2동 서광아파트 102동 807호	
【국적】	KR	
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 정홍식 (인)	
【수수료】		
【기본출원료】	20	면 29,000 원
【가산출원료】	8	면 8,000 원
【우선권주장료】	0	건 0 원
【심사청구료】	0	항 0 원
【합계】	37,000 원	
【첨부서류】	1. 요약서·명세서(도면)_1통	

**【요약서】****【요약】**

홈 디바이스에 대한 인증시스템 및 인증방법이 개시된다. 홈 디바이스의 인증시스템은, 인증을 수행하기 위한 암호화 정보 및 인증서비스를 제공하는 서비스 제공자 정보를 가지는 홈 디바이스와, 홈 디바이스의 암호화 정보에 대응하는 복호화 정보를 제공하는 서비스 제공자, 및 홈 디바이스가 물리적으로 연결되는 경우 상기 서비스 제공자 정보를 이용해 서비스 제공자에 상기 복호화 정보를 요청하고 홈 디바이스의 인증을 수행하는 홈 게이트웨이를 갖는다. 따라서 홈 네트워크의 프라이버시 및 시큐러티를 보장한다.

**【대표도】**

도 2

**【색인어】**

홈 네트워크, 홈 디바이스, 인증, 암호화

**【명세서】****【발명의 명칭】**

홈 디바이스의 인증시스템 및 그의 인증방법{Authentication system of home device and a method authenticating thereof }

**【도면의 간단한 설명】**

도 1은 종래의 일반적인 홈 네트워크 시스템에 대한 개념도,

도 2는 본 발명에 따른 홈 디바이스의 인증시스템에 대한 개략적인 구성도,

도 3은 본 발명에 따른 디바이스(311)내에 포함된 디바이스 정보(DI)를 예시한 도,

도 4는 본 발명에 따른 홈 게이트웨이(330)의 상세한 블록도,

도 5는 본 발명에 따른 홈 게이트웨이(330)의 디바이스 처리부(333)에 대한 상세한 블록도,

도 6은 본 발명에 따른 새로운 디바이스에 대한 승인여부 요청화면(600)을 예시한 도,

그리고

도 7은 본 발명에 따른 홈 디바이스 인증방법에 대한 흐름을 도시한 도이다.

\* 도면의 주요부분에 대한 부호의 설명 \*

300 : 홈 네트워크      330 : 홈 게이트웨이(HG)

331 : 입출력부      333 : 디바이스 처리부

335 : 응용처리부      337 : 표시부

339 : 사용자입력부      333-1 : 정보검출부

333-2 : 인증처리부 333-3 : 선택부

333-4 : 정보저장부 400 : 서비스제공자

### 【발명의 상세한 설명】

#### 【발명의 목적】

#### 【발명이 속하는 기술분야 및 그 분야의 종래기술】

- <15> 본 발명은 홈 네트워크 시스템에 관한 것으로서, 보다 상세하게는 홈 네트워크 시스템의 시큐러티를 위해 홈 디바이스의 인증과정을 수행하는 홈 디바이스 인증시스템 및 그의 인증방법에 관한 것이다.
- <16> 최근 인터넷의 발달과 함께 xDSL이나, 혹은 케이블 모뎀(cable modem)등이 많은 가정에 보급되어 고속의 인터넷 액세스가 가능하게 되었으며, 이에 따라서 가정내의 PC에서 인터넷으로 접속을 폭발적으로 증가시켰다.
- <17> 사용자는 이제 인터넷 접속만으로 만족하지 않고 PC를 통해 가정내의 디바이스를 제어하고 통신할 수 있기를 기대하고 있으며, 동시에 가정 바깥에서 조차 가정내 디바이스와 통신하여 새로운 서비스를 제공받을 수 있는 홈 네트워크 시스템이 개발되고 있다.
- <18> 홈 네트워크 시스템은 일반적으로 PC를 비롯한 가정내 정보가전기기들이 하나의 네트워크로 통합되어 통신이 가능하도록 함을 일컫는다. 홈 네트워크 시스템은 네트워킹기술, 기반소프트웨어 그리고 정보 가전기기의 발전에 따라 급속히 확산되고 있다.
- <19> 이와 같은 홈 네트워크 시스템의 구축은, 기존에 가정내에 구축된 전화선(Home PNA: Home Phoneline Networking Alliance), 전원 콘센트(전등선 LAN), 및 TV의 동축케이블 등의 배선을 활용하고 있으며, 도 1은 이러한 홈 네트워크 시스템에 대한 개념도이다.

<20> 제1 및 제2 홈 네트워크(100,200)내에는 제1 및 제2 홈 게이트웨이(110,210)가 구비된다. 제1 및 제2홈 게이트웨이(110,210))에는 각각의 홈디바이스(111,113,115,117)(211,213)가 상호 연결되어 네트워킹하며, 제1 및 제2 홈 게이트웨이(110)(210)를 통해 외부 네트워크과 접속된다.

<21> 이와 같은 종래의 홈 네트워크에서는, 새로운 디바이스를 홈 네트워크에 연결할 경우, 일반적으로 디바이스에 대한 인증절차가 없었다. 즉, 제1홈 네트워크(100)내의 새로운 디바이스(113)를 연결할 경우, 새로운 디바이스(113)는 제1홈 게이트웨이(110)에 물리적으로 접속하여 접속정보를 전송함으로써 새로운 디바이스(113)는 제1홈게이트웨이(110)에 연결된다. 이와 같이, 제1홈게이트웨이(110)에서만 새로운 디바이스(113)를 인증하는 단방향성 구조를 갖는다. 이에 의해, 제1홈 네트워크(100)와 인접한 제2홈 네트워크(200)의 제2홈 게이트웨이(210)에도 전화선, 전등선 LAN, 및 TV의 동축케이블 등과 같은 배선에 의해 새로운 디바이스(113)의 접속 정보가 전송되게 된다. 따라서, 우연히든, 혹은, 의도적이든 제1홈 네트워크(100)의 홈 디바이스(113)는 제2홈 네트워크에 연결되며, 이에 의해 제1홈 네트워크(100)는 제2홈 네트워크에 노출되게 된다.

<22> 이상과 같이, 종래의 홈 네트워크내에 연결되는 홈 디바이스에 대한 인증과정이 없으므로, 프라이버시(Privacy) 및 시큐러티(Security)에 대한 문제점을 갖고 있다.

#### 【발명이 이루고자 하는 기술적 과제】

<23> 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 홈 네트워크의 프라이버시 및 시큐러티를 위해 홈 디바이스의 인증과정을 수행하는 홈 디바이스 인증시스템 및 그의 인증방법에 관한 것이다.

### 【발명의 구성 및 작용】

- <24> 상기 목적을 달성하기 위한 본 발명에 따른 홈 디바이스의 인증시스템은, 인증을 수행하기 위한 암호화 정보 및 인증서비스를 제공하는 서비스 제공자 정보를 포함하는 디바이스 정보를 가지는 홈 디바이스; 상기 홈 디바이스의 상기 암호화 정보에 대응하는 복호화 정보를 제공하는 서비스 제공자; 및 상기 서비스 제공자 정보를 이용해 상기 서비스 제공자에 상기 복호화 정보를 요청하고, 상기 홈 디바이스의 인증을 수행하는 홈 게이트웨이;를 갖는다.
- <25> 상기 홈 게이트웨이는, 상기 암호화 정보 및 상기 서비스 제공자 정보를 포함하는 디바이스 정보가 입력되는 입출력부; 상기 서비스 제공자 정보를 이용해 상기 복호화 정보를 획득하고, 획득한 상기 복호화 정보 및 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고, 수행된 인증결과를 디스플레이하기 위한 소정의 디스플레이 디바이스를 선택하는 디바이스 처리부; 및 상기 인증결과에 대한 사용자의 승인여부를 요청하는 승인여부 요청화면을 생성하는 응용처리부;를 갖는다.
- <26> 상기 입출력부는, 상기 승인여부 요청화면을 선택된 상기 디스플레이 디바이스로 출력하며, 상기 디바이스 처리부는, 상기 승인여부 요청화면을 통한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하도록 상기 입출력부를 제어한다.
- <27> 상기 홈 게이트웨이는, 상기 인증결과를 사용자에게 알리는 표시부; 및 상기 표시부에 표시되는 상기 인증결과에 대응하여 승인 여부에 대한 사용자의 선택명령이 입력되는 사용자입력부;를 더 갖는다.

- <28> 상기 디바이스 처리부는, 사용자 입력부로부터 입력되는 사용자의 선택명령에 대응하여 상기 디바이스 처리부는 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하도록 상기 입출력부를 제어한다.
- <29> 상기 디바이스 처리부는, 소정 시간 동안 상기 사용자의 승인 여부 결정에 대한 응답신호가 입력되지 않으면, 상기 홈 네트워크 상에 상기 홈 디바이스가 셋팅되는 것을 차단하도록 상기 입출력부를 제어한다.
- <30> 상기 디바이스 처리부는, 상기 입출력부로부터 입력된 상기 암호화 정보 및 상기 서비스 제공자 정보를 검출하는 정보 검출부; 상기 복호화 정보와 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고, 상기 승인여부 요청화면에 의한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 제어하는 인증 처리부; 상기 홈 네트워크에 연결된 각각의 홈 디바이스의 정보가 저장되는 정보 저장부; 및 기저장된 상기 각각의 홈 디바이스 정보에 기초하여 상기 인증 처리부에서 수행된 인증결과에 대한 디스플레이가 가능한 디바이스를 선택하는 선택부;를 갖는다.
- <31> 상기 사용자의 승인여부에 따라서 상기 홈 네트워크상에 상기 홈 디바이스의 셋팅이 승인되는 경우, 상기 인증 처리부는 상기 홈 디바이스의 정보를 상기 정보 저장부에 저장시킨다.
- <32> 본 발명에 따른 홈 디바이스의 인증방법은, 인증을 수행하기 위한 암호화 정보 및 인증 서비스를 제공하는 서비스 제공자 정보를 포함하는 디바이스 정보가 입력되는 단계; 상기 서비스 제공자 정보를 이용해 서비스 제공자에 복호화 정보를 요청하고 요청받은 상기 복호화 정보 및 상기 암호화 정보를 이용해 상기 홈 디바이스의 인증을 수행하고 수행된 인증결과가 디스

플레이 가능한 디바이스를 선택하는 디바이스 처리단계; 및 상기 인증결과에 대한 사용자의 승인여부를 요청하는 승인여부 요청화면을 생성하는 단계;를 가지는 것을 특징으로 한다.

<33> 생성된 상기 승인여부 요청화면을 상기 디스플레이 디바이스로 출력하는 단계; 및 상기 승인여부 요청화면을 통한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하는 단계;를 더 가지는 것을 특징으로 한다.

<34> 상기 인증결과를 사용자에게 알리는 표시단계; 및 상기 표시단계에 표시되는 상기 인증결과에 대응하여 승인 여부에 대한 사용자의 선택명령이 입력되는 사용자 입력단계;를 더 가지는 것을 특징으로 한다.

<35> 상기 홈 디바이스 셋팅여부를 수행하는 단계는, 사용자 입력단계로부터 입력되는 사용자의 선택명령에 대응하여 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행한다.

<36> 상기 홈 디바이스의 셋팅여부를 수행하는 단계는, 소정 시간 동안 상기 사용자의 승인여부 결정에 대한 응답신호가 입력되지 않으면, 상기 홈 네트워크 상에 상기 홈 디바이스가 셋팅되는 것을 차단한다.

<37> 상기 디바이스 처리단계는, 입력된 상기 암호화 정보 및 상기 서비스 제공자 정보를 포함하는 상기 디바이스 정보를 검출하는 검출단계; 상기 복호화 정보와 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고, 상기 승인여부 요청화면에 의한 사용자의 승인여부에 따라서 홈 네트워크상에 상기 홈 디바이스의 셋팅여부를 제어하는 인증처리단계; 및 상기 홈 네트워크에 연결된 각각의 홈 디바이스의 정보에 기초하여 상기 인증처리단계에서 수행된 인증결과에 대한 디스플레이가 가능한 디바이스를 선택하는 선택단계;를 가지는 것을 특징으로 한다.

- <38> 바람직하게는, 상기 사용자의 승인여부에 따라서 상기 홈 네트워크상에 상기 홈디바이스의 셋팅이 승인되는 경우, 상기 홈 디바이스의 정보를 저장하는 단계;를 더 가지는 것을 특징으로 한다.
- <39> 따라서, 홈 네트워크에 연결되는 디바이스의 인증절차를 수행함에 따라서 우연히, 혹은 고의적으로 연결되는 다른 네트워크내의 디바이스의 접속을 막을 수 있다. 이에 의해 네트워크 시스템의 프라이버시 및 시큐러티를 보장할 수 있다. 또한, 홈 네트워크 환경이 익숙하지 않은 사용자에게 보다 편리한 방법으로 홈 디바이스를 설치/등록 할 수 있다.
- <40> 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.
- <41> 도 2는 본 발명에 따른 홈 디바이스 인증시스템에 대한 설명을 위한 개념도이다.
- <42> 홈 디바이스의 인증시스템은 홈 네트워크(300)에 새롭게 연결되는 홈 디바이스(311)와, 홈 네트워크(300)의 서버기능을 수행하는 홈 게이트웨이(330), 및 새로운 디바이스(New device:311)의 인증을 수행하기 위한 소정의 암호화 정보를 제공하는 서비스 제공자(400)를 갖는다.
- <43> 먼저, 본 발명에 따른 홈 디바이스(311)는, 도 3에 도시된 바와 같은 디바이스 정보(DI)를 갖는다. 디바이스 정보(DI)는, 일반적인 디바이스 사항정보(I1), 디바이스의 인증서비스를 제공하는 서비스 제공자 정보(I2), 및 디바이스의 인증절차를 수행하기 위한 소정의 암호화 정보(I3) 등을 갖는다.
- <44> 홈 게이트웨이(330)는 도 4에 도시된 바와 같이, 홈 네트워크 상의 홈 디바이스들과 다양한 유무선을 통해 연결되어 DHCP(Dynamic Host Configuration Protocol)와 같은 네트워크 프로토콜을 통해 전송되는 데이터의 입력 및 출력이 수행되는 입출력부(331), 새로운 디바이스

(311)에 대한 인증처리를 수행하기 위한 디바이스 처리부(333), 디바이스 인증서비스를 제공하기 위한 소정의 응용프로그램을 적용시키는 응용처리부(335), 사용자에게 인증결과에 대응하는 소정의 정보를 알려주는 예컨데, LED 와 같은 표시부(337), 및 사용자의 조작명령이 입력되는 예컨데, 조작패널인 사용자입력부(339) 등을 갖는다.

<45> 서비스 제공자(400)는 홈 게이트웨이(330)에 연결되는 새로운 디바이스(311)의 인증을 수행하기 위해 홈 게이트웨이(330)에서 요청된 새로운 디바이스(311)에 대응하는 소정의 암호화 정보를 홈 게이트웨이(330)에 제공한다.

<46> 도 5는 본 발명에 따른 홈 게이트웨이(330)의 디바이스 처리부(333)에 대한 상세한 블록도이며, 도 4 및 도 5를 참조하여 디바이스 처리부(333)의 동작을 상세하게 설명한다.

<47> 디바이스 처리부(333)는 정보 검출부(333-1), 인증 처리부(333-2), 선택부(333-3) 및 정보 저장부(333-4) 등을 가지고 있다.

<48> 정보 검출부(333-1)는 새로운 디바이스(311)가 홈 네트워크에 물리적으로 연결되었을 경우, 입출력부(331)로부터 입력되는 새로운 디바이스(311) 정보에 기초하여 새로운 디바이스가 연결되었음을 인식하고 입력되는 도 3에 도시된 바와 같은, 디바이스 정보(DI)를 검출한다.

<49> 인증 처리부(333-2)는 소정의 인증알고리즘을 이용하여 새로운 디바이스(311)의 인증을 수행한다. 즉, 새로운 디바이스(311)에 대한 디바이스 정보(DI) 중 인증을 위해 마련된 정보, 예를 들면, 도 3에 도시된 디바이스 정보(DI) 중 서비스 제공자 정보(I2) 및 암호화 정보(I3)를 이용하여 새로운 디바이스(311)의 인증절차를 수행한다.

<50> 인증알고리즘으로 예컨데, 공개키(Public Key) 알고리즘 및 해쉬(Hash) 알고리즘을 이용하여 인증을 수행하는 경우를 예로서 설명한다. 먼저, 인증 처리부(333-2)는 디바이스 정보

(DI) 중 서비스 제공자 정보(I2)를 이용하여 서비스 제공자 측에 해당하는 디바이스의 공개키를 요청한다. 인증 처리부(333-2)는 서비스 제공자측으로부터 공개키를 제공 받으면, 공개키를 이용하여 암호화 정보(I3)의 시그너쳐(Signature)를 복호화 한다. 여기서, 시그너쳐는 소정의 메시지를 해쉬로 단축하여 해쉬값을 구하고, 구해진 해쉬값을 개인키(Private Key)으로 암호한 것이다. 즉, 공개키를 이용하여 개인키인 시그너쳐를 복호화하여 원래의 해쉬값을 복원하게 된다. 따라서, 소정의 메시지의 해쉬값을 구하여 복원된 해쉬값과 비교함으로써 소정의 메시지가 정상적인지의 여부를 판단한다.

<51> 정보 저장부(333-4)는 홈 게이트웨이(330)에 연결된 각각의 홈 디바이스에 대한 정보 등이 저장된다.

<52> 선택부(333-3)는 정보 저장부(333-4)에 저장된 홈 네트워크 상의 각각의 디바이스의 정보를 검색하여 이하 설명되는 승인여부 요청화면을 디스플레이할 수 있는 최적의 디스플레이 디바이스를 선택한다. 예를 들면, 가장 최근에 사용된 디스플레이 가능한 디바이스를 선택한다.

<53> 이와 같이, 인증 처리부(333-2)에서 처리된 인증결과 및 선택부(333-3)에서 선택된 디스플레이 가능한 디바이스의 정보를 홈 게이트웨이(330)의 응용처리부(335)에 제공한다. 응용처리부(335)에서는 사용자에게 인증결과(A1) 및 이에 따른 디바이스 승인여부(A2)를 요청하는 도 6에 도시된 바와 같은, 승인여부 요청화면(600)을 생성한다. 이렇게 생성된 승인여부 요청화면(600)은 선택된 디스플레이 디바이스에 전송되며 사용자는 디스플레이된 승인여부 요청화면(600)을 통해 사용자는 새로운 디바이스(311)의 승인여부를 결정하게 된다.

- <54> 만일, 승인여부 요청화면(600)을 디스플레이 할 수 있는 디바이스가 현재 홈네트워크 상에 존재하지 않을 경우에는 홈 게이트웨이(330)의 표시부(LED)(337) 및 사용자입력부(339)를 통해 승인여부를 결정하게 된다.
- <55> 예를 들어, 홈 게이트웨이(330)에 새롭게 연결된 디바이스(311)가 인증 처리부(333-2)에서 합법적인 디바이스로 인증된 경우에는 청색의 LED(337)를, 반대로, 새로운 디바이스(311)의 인증결과가 합법적이지 못한 비정상적인 디바이스인 경우에는 적색의 LED(337)를 발광시켜 인증결과를 사용자에게 알린다. 이에 의해 사용자는 사용자입력부(339)를 통해 승인여부를 결정하게 된다.
- <56> 이와 같이, 사용자의 승인여부에 따라서 새로운 디바이스(311)의 홈 네트워크에 셋팅여부가 결정됨으로써 홈 네트워크의 프라이버시 및 시큐러티가 보장되며, 또한, 사용자에게 홈 디바이스의 설치/등록에 대한 서비스를 제공하게 되어 사용상의 편의성을 도모할 수 있다.
- <57> 이하에서는 도 7의 홈 디바이스 인증과정에 대한 흐름도를 참조하여 홈 네트워크상에 새롭게 연결되는 홈 디바이스의 인증과정을 보다 상세하게 설명한다.
- <58> 먼저, 새로운 디바이스(311)는 홈 게이트웨이(330)와 물리적으로 연결되며, 이때 새로운 디바이스의 제조사로부터 받은 디바이스 정보(DI)를 DHCP 방송 메시지(broadcast message)와 같은 형태로 입출력부(331)에 전송된다.
- <59> 정보 검출부(333-1)는 홈 게이트웨이(330)의 입출력부(331)에 입력되는 새로운 디바이스(311)의 디바이스 정보(DI)에 따라 새로운 디바이스(311)가 연결됨을 인식하고 디바이스 정보(도 3에 예시된 디바이스 정보: DI)를 검출한다.
- <60> 정보 검출부(333-1)에서 검출된 디바이스 정보(DI)를 인증 처리부(333-2)에 전송한다.

- <61> 인증 처리부(333-2)는 디바이스 정보(DI)를 이용하여 새로운 디바이스의 인증을 수행한다. 예컨데, 인증 서비스 제공자 정보(I2)를 이용해 서비스 제공자측에 공개키를 요청한다. 공개키를 서비스 제공자측에 요청였으나, 등록되지 않은 디바이스이거나, 디바이스 정보가 초기 서비스 제공자의 것과 다른 경우, 적법한 디바이스가 아닌 것으로 판단하여 네트워크에 셋팅되는 것을 차단한다.
- <62> 한편, 인증 처리부(333-2)는 서비스 제공자측으로부터 제공 받은 공개키(Public Key)를 이용하여 암호화 정보(I3)인 시그너쳐(Signature)를 복호화하여 해쉬값을 복원한다. 복원된 해쉬값과 구해진 해쉬값을 각각 비교하여 정상적인 디바이스 정보인지의 여부를 판단한다.
- <63> 선택부(333-3)는 정보 저장부(333-4)에 저장된 홈 네트워크의 디바이스의 정보에 기초하여 승인여부 요청화면(600)을 디스플레이 할 수 있는 최적의 디스플레이 디바이스, 예컨데, 가장 최근에 사용된 디스플레이 디바이스를 선택한다.
- <64> 응용 처리부(333)에는 인증 처리부(333-2)에서 처리된 인증결과 및 선택부(333-3)에서 선택된 디스플레이 디바이스의 정보가 전송되어 도 6에 도시된 바와 같은 승인여부 요청화면(600)을 생성한다. 승인여부 요청화면(600)은 선택된 디스플레이 디바이스로 표시되어 사용자에 의해 새로운 디바이스의 승인여부가 결정된다.
- <65> 사용자는 승인여부 요청화면(600)에 표시되는 인증결과를 포함하는 디바이스의 정보에 기초하여 디바이스의 승인여부를 결정한다. 예컨데, 새로운 디바이스(311)의 인증결과가 합법적인 정상적인 디바이스인 경우 사용자는 'YES'를 선택하여 새로운 디바이스(311)가 네트워크에 셋팅되는 것을 승인한다. 승인신호 'YES'는 홈 게이트웨이(330)의 응용 처리부(335)에 전송되고, 응용 처리부(335)는 승인신호 'YES'에 대응하는 새로운 디바이스(311)의 등록신호를 인증 처리부(333-2)에 전송한다. 이에 의해 인증 처리부(333-2)는 새로운 디바이스(311)의 디바

이스 정보를 정보 저장부(333-4)에 저장하고, 새로운 디바이스(311)의 네트워크 셋팅을 진행하도록 입출력부(331)를 제어한다.

<66> 한편, 새로운 디바이스(311)의 인증결과가 합법적이지 못한 비정상적인 디바이스인 경우에는 사용자는 'NO'를 선택하여 새로운 디바이스(311)가 네트워크에 셋팅되는 것을 막는다. 또는, 소정 시간 동안 승인여부에 대한 사용자의 응답신호가 없는 경우 새로운 디바이스(311)의 네트워크 셋팅은 자동적으로 차단된다.

<67> 승인을 거절하는 거절신호인 'NO'가 입력되거나, 소정 시간 동안 사용자의 응답신호가 없는 경우, 응용 처리부(335)는 새로운 디바이스(311)에 대한 승인거절신호를 인증 처리부(333-2)에 전송한다. 인증 처리부(333-2)는 새로운 디바이스(311)가 네트워크에 셋팅되지 않도록 입출력부(331)를 제어한다.

<68> 상기와 같은 홈 디바이스 인증시스템에 의해, 새로운 디바이스가 홈 네트워크에 등록되는 과정에서 소정의 암호와 알고리즘에 의해 인증절차를 거친 후, 사용자의 승인여부에 따라서 네트워크에 등록여부가 결정된다. 따라서, 홈 네트워크의 프라이버시 및 시큐러티가 보장될 수 있다.

### 【발명의 효과】

<69> 본 발명에 따르면, 첫째, 홈 네트워크에 연결되는 디바이스의 인증절차를 수행함에 따라서 우연히, 혹은 고의적으로 연결되는 다른 네트워크내의 디바이스의 접속을 막을 수 있다. 이에 의해 네트워크 시스템의 프라이버시 및 시큐러티를 보장할 수 있다.

<70> 둘째, 홈 네트워크 환경이 익숙하지 않은 사용자에게 보다 편리한 방법으로 홈 디바이스를 설치/등록 할 수 있다.

<71> 이상에서는 본 발명의 바람직한 실시예에 대해서 도시하고 설명하였으나, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

**【특허청구범위】****【청구항 1】**

인증을 수행하기 위한 암호화 정보 및 인증서비스를 제공하는 서비스 제공자 정보를 포함하는 디바이스 정보를 가지는 홈 디바이스;

상기 홈 디바이스의 상기 암호화 정보에 대응하는 복호화 정보를 제공하는 서비스 제공자; 및

상기 서비스 제공자 정보를 이용해 상기 서비스 제공자에 상기 복호화 정보를 요청하고, 상기 홈 디바이스의 인증을 수행하는 홈 게이트웨이;를 포함하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 2】**

제 1항에 있어서,

상기 홈 게이트웨이는,

상기 암호화 정보 및 상기 서비스 제공자 정보를 포함하는 디바이스 정보가 입력되는 입출력부;

상기 서비스 제공자 정보를 이용해 상기 복호화 정보를 획득하고, 획득한 상기 복호화 정보 및 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고, 수행된 인증결과를 디스플레이하기 위한 소정의 디스플레이 디바이스를 선택하는 디바이스 처리부; 및

상기 인증결과에 대한 사용자의 승인여부를 요청하는 승인여부 요청화면을 생성하는 응용처리부;를 포함하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 3】**

제 2항에 있어서,

상기 입출력부는, 상기 승인여부 요청화면을 선택된 상기 디스플레이 디바이스로 출력하며,

상기 디바이스 처리부는, 상기 승인여부 요청화면을 통한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하도록 상기 입출력부를 제어하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 4】**

제 2항에 있어서,

상기 홈 게이트웨이는,

상기 인증결과를 외부에 표시하는 표시부; 및  
표시된 상기 인증결과에 대응하여 승인 여부에 대한 사용자의 선택명령이 입력되는 사용자입력부;를 더 포함하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 5】**

제 2항에 있어서,

상기 디바이스 처리부는,

사용자 입력부로부터 입력되는 사용자의 선택명령에 대응하여 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하도록 상기 입출력부를 제어하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 6】**

제 2항에 있어서,

상기 디바이스 처리부는,

소정 시간 동안 상기 사용자의 승인여부에 대한 응답신호가 입력되지 않으면, 홈 네트워크 상에 상기 홈 디바이스가 셋팅되는 것을 차단하도록 상기 입출력부를 제어하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 7】**

제 2항에 있어서,

상기 디바이스 처리부는,

상기 입출력부로부터 입력된 상기 암호화 정보 및 상기 서비스 제공자 정보를 검출하는 정보 검출부;

상기 복호화 정보와 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고, 상기 승인여부 요청화면에 의한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 제어하는 인증 처리부;

상기 홈 네트워크에 연결된 각각의 홈 디바이스의 정보가 저장되는 정보 저장부; 및 기저장된 상기 각각의 홈 디바이스 정보에 기초하여 상기 인증 처리부에서 수행된 인증 결과에 대한 디스플레이가 가능한 디바이스를 선택하는 선택부;를 포함하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

**【청구항 8】**

제 7항에 있어서,

상기 사용자의 승인여부에 따라서 상기 홈 네트워크상에 상기 홈 디바이스의 셋팅이 승인되는 경우,

상기 인증 처리부는 상기 홈 디바이스의 정보를 상기 정보 저장부에 저장시키는 것을 특징으로 하는 홈 디바이스의 인증시스템.

#### 【청구항 9】

인증을 수행하기 위한 암호화 정보 및 인증서비스를 제공하는 서비스 제공자 정보를 포함하는 디바이스 정보가 입력되는 단계;

상기 서비스 제공자 정보를 이용해 서비스 제공자에 복호화 정보를 요청하고, 요청받은 상기 복호화 정보 및 상기 암호화 정보를 이용해 상기 홈 디바이스의 인증을 수행하고, 수행된 인증결과가 디스플레이 가능한 디바이스를 선택하는 디바이스 처리단계; 및

상기 인증결과에 대한 사용자의 승인여부를 요청하는 승인여부 요청화면을 생성하는 단계;를 포함하는 것을 특징으로 하는 홈 디바이스의 인증방법.

#### 【청구항 10】

제 9항에 있어서,

생성된 상기 승인여부 요청화면을 상기 디스플레이 디바이스로 출력하는 단계; 및  
상기 승인여부 요청화면을 통한 사용자의 승인여부에 따라서 홈 네트워크 상에 상기 홈 디바이스의 셋팅여부를 수행하는 단계;를 더 포함하는 것을 특징으로 하는 홈 디바이스의 인증 방법.

#### 【청구항 11】

제 9항에 있어서,

상기 인증결과를 외부에 표시하는 표시단계; 및  
표시된 상기 인증결과에 대응하여 승인 여부에 대한 사용자의 선택명령이 입력되는 사용  
자 입력단계;를 더 포함하는 것을 특징으로 하는 홈 디바이스의 인증시스템.

#### 【청구항 12】

제 10항에 있어서,

상기 홈 디바이스 셋팅여부를 수행하는 단계는,

사용자 입력단계에서 입력된 사용자의 선택명령에 대응하여 홈 네트워크 상에 상기 홈  
디바이스의 셋팅여부를 수행하는 것을 특징으로 하는 홈 디바이스의 인증방법.

#### 【청구항 13】

제 10항에 있어서,

상기 홈 디바이스의 셋팅여부를 수행하는 단계는,

소정 시간 동안 상기 사용자의 승인여부에 대한 응답신호가 입력되지 않으면, 상기 홈  
네트워크 상에 상기 홈 디바이스의 셋팅을 차단시키는 것을 특징으로 하는 홈 디바이스의 인증  
방법.

#### 【청구항 14】

제 9항에 있어서,

상기 디바이스 처리단계는,

입력된 상기 암호화 정보 및 상기 서비스 제공자 정보를 포함하는 상기 디바이스 정보를  
검출하는 검출단계;

상기 복호화 정보와 상기 암호화 정보를 이용하여 상기 홈 디바이스의 인증을 수행하고  
상기 승인여부 요청화면에 의한 사용자의 승인여부에 따라서 홈 네트워크상에 상기 홈 디바  
이스의 셋팅여부를 제어하는 인증처리단계; 및

상기 홈 네트워크에 연결된 각각의 홈 디바이스의 정보에 기초하여 상기 인증처리단계에  
서 수행된 인증결과에 대한 디스플레이가 가능한 디바이스를 선택하는 선택단계;를 포함하는  
것을 특징으로 하는 홈 디바이스의 인증방법.

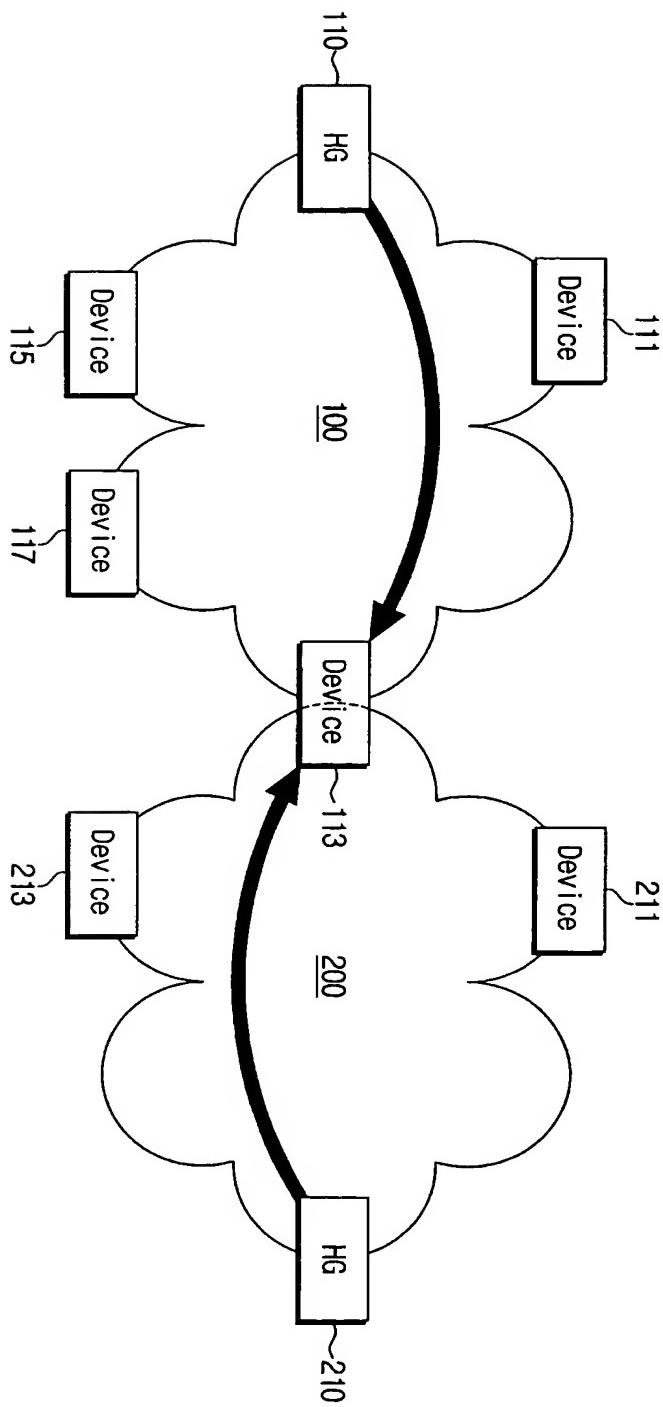
#### 【청구항 15】

제 14항에 있어서,

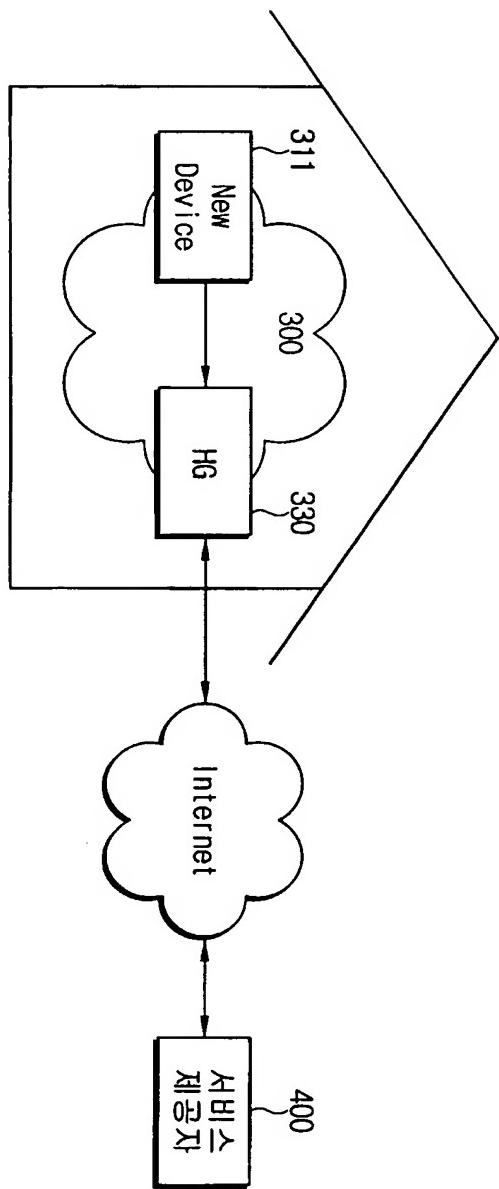
상기 사용자의 승인여부에 따라서 상기 홈 네트워크상에 상기 홈디바이스의 셋팅이 승인  
되는 경우, 상기 홈 디바이스의 정보를 저장하는 단계;를 더 포함하는 것을 특징으로 하는 홈  
디바이스의 인증방법.

【도면】

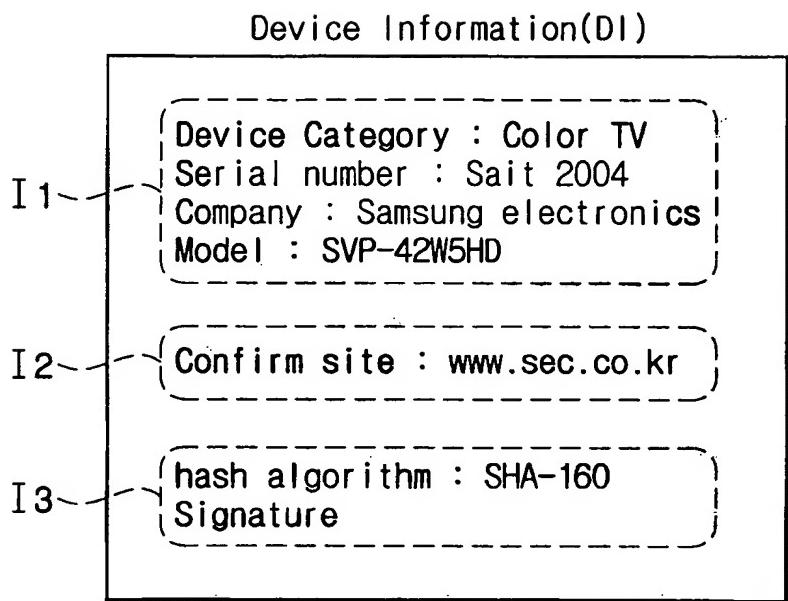
【도 1】



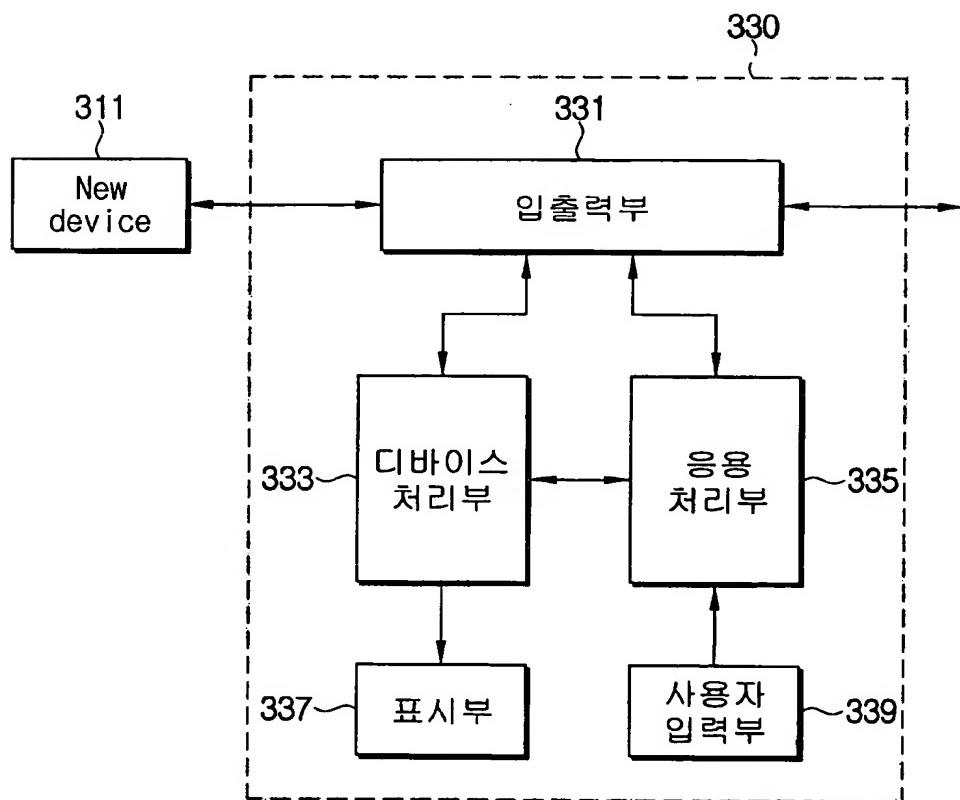
【도 2】



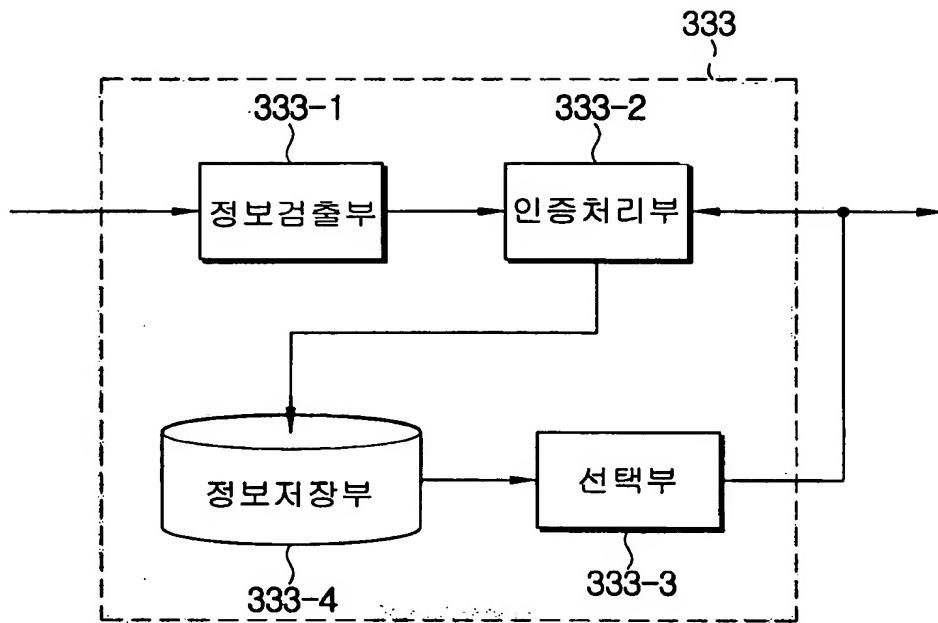
## 【도 3】



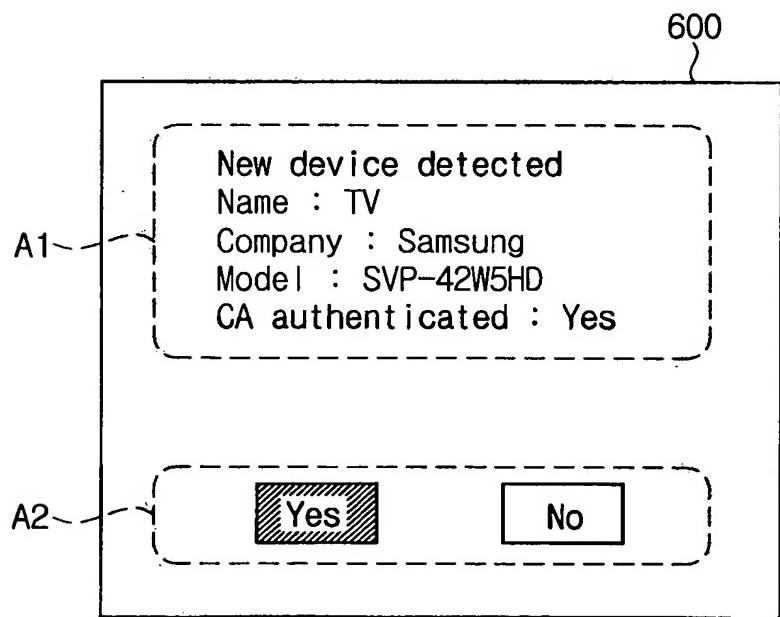
## 【도 4】



【도 5】



【도 6】



【도 7】

